2010-12

Managing the aviation insider threat

Black, Alan

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

MANAGING THE AVIATION INSIDER THREAT

by

Alan Black

December 2010

Thesis Co-Advisors: Richard Bergin
Robert Josefek

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Managing the Aviation Insider Threat			**5. FUNDING NUMBERS**
6. AUTHOR(S) Alan Black			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number _____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Despite enhancements to aviation security since September 11, 2001, there remain vulnerabilities from employees at airports. This threat results from airline/airport employees that have access to sensitive and restricted areas during the normal course of their required duties. This thesis evaluates the threat and the measures in place to prevent attacks from aviation insiders. In addition, it evaluates a measure commonly referred to as 100 percent employee screening. Finally, the thesis derives recommendations to enhance the current methods to reduce the vulnerability, as well as proposes additional measures to further reduce the threat from aviation insiders.

14. SUBJECT TERMS aviation insider, insider threat, aviation vulnerabilities, 100 percent employee screening, aviation security, finger print based criminal history records check, employee background checks			**15. NUMBER OF PAGES** 79
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

MANAGING THE AVIATION INSIDER THREAT

Alan Black
Vice President and Director of Public Safety, Dallas Fort Worth International Airport,
Department of Public Safety, Texas
B.A., Western Illinois University, 2005

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2010

Author: Alan Black

Approved by: Richard Bergin
Thesis Co-Advisor

Robert Josefek
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Despite enhancements to aviation security since September 11, 2001, there remain vulnerabilities from employees at airports. This threat results from airline/airport employees that have access to sensitive and restricted areas during the normal course of their required duties. This thesis evaluates the threat and the measures in place to prevent attacks from aviation insiders. In addition, it evaluates a measure commonly referred to as 100 percent employee screening. Finally, the thesis derives recommendations to enhance the current methods to reduce the vulnerability, as well as proposes additional measures to further reduce the threat from aviation insiders.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AAAE	American Association of Airport Executives
ACO	Access Control Office
ATSSP	Aviation Transportation System Security Plan
CBP	Customs and Border Protection
CCTV	Close Circuit Television
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
DFW	Dallas Fort Worth International Airport
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FIS	Federal Inspection Station
GAO	Government Accountability Office
LAX	Los Angeles World Airport
NSAS	National Strategy for Aviation Security
OIS	Office of Intelligence
SIDA	Security Identification Display Area
STA	Security Threat Assessment
TIG	Transportation Intelligence Gazette
TSA	Transportation Security Administration
U/FOUO	Unclassified/For Official Use Only
U.S.	United States

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Completing this research would not have been possible without the love and support of my wife, Vicky. Along with me, she endured the long hours and endless work with love and patience. She inspires me.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Despite many enhancements to aviation security since September 11, 2001, there remain vulnerabilities from the insider threat (Transportation Security Administration [TSA], 2009). This threat results from the risk that results when malicious airline/airport employees have access to sensitive and restricted areas during the normal course of their required duties. This may include pilots, aircraft mechanics, aircraft fuelers and cleaners, and airline or contract employees who load baggage. It may also include airport staff such as police officers and firefighters. Physical barriers are in place to inhibit unauthorized entry into restricted areas; however, certain vulnerabilities continue to exist once the employee is through the physical barriers.

The purpose of this thesis is to provide situational awareness of a vulnerability that exists within the commercial aviation domain and to advocate swift implementation of the actions necessary to significantly strengthen its resistance to the insider threat.

A. BACKGROUND

Aviation security in a post-9/11 world has been significantly improved. The improvements have focused on reducing the threat of attack primarily through managing commercial aviation passengers, including increased passenger screening criteria, aircraft cockpit door hardening and the vetting of passengers through various Department of Homeland Security and the Department of Justice "watch-lists."[1] However, the threat from an attack by an insider has not been adequately addressed.

The aviation security environment is susceptible to an attack by the very people who are employed to make commercial aviation a thriving business. Commercial aviation employees have access to secure areas in U.S. airports that would offer them the unique ability to silently attack a commercial aircraft by overt or covert means. Aviation

[1] A watch list is a list of names used to compare passenger identification against a list of individuals known or suspected to be engaged in activities contradictory to aviation security.

employees, insiders with the proper motivation and equipment, could plant explosives, weapons or disable critical aircraft components that could cause large loss of life and business disruption to the U.S. economy.

Over the last few decades and particularly since the terrorists' attacks on U.S. aviation on September 11, 2001, the focus of U.S. aviation defensive posture has been on the commercial airline passenger. This was a natural reaction to the most popular form of attack by terrorists. Passenger identification and screening has undergone continuous modifications following each attack or attempted attack. The hardening of cockpits doors was a direct reaction to the attacks of September 11, 2001 in order to maintain the security of the cockpit. Furthermore, carrying large quantities of liquids through airport screening was implemented following a plan to use volatile liquids to explode airliners over the Atlantic in 2006. With the somewhat singular attention given to airline passengers by security experts, it is important to consider other threats and to work toward understanding and forecasting the next vulnerability that terrorists will attempt to exploit. Devoted terrorists will not simply give up the fight based on the fact that getting direct access to commercial aircraft as a passenger has become more difficult. Terrorists will begin to explore other methods, where they find the least resistance, to carry out their attacks.

One such vulnerability would be to either have a terrorist operative become an employee of an airline, thus having unescorted access in and around the aircraft or the opportunity to corrupt an incumbent employee into providing access or to act as an agent of the terrorist.

While the number of terrorist related incidents involving insiders, such as the one above, is somewhat limited, there are a large number of incidents where insiders used their special airport access to conduct criminal behaviors. Those behaviors include drug trafficking, human smuggling, and weapons smuggling. There is clear potential for airport/airline employees involved in criminal activity to become, directly or indirectly, involved with terrorism and terrorist groups. Should the insiders not be inspired for ideological reasons, they could be convinced for financial reasons.

Although the insider threat affects local environments at individual airports, the challenges, as well as the solutions, are much broader and impact the entire aviation system, various local law-enforcement organizations, private-sector air carriers, and federal agencies responsible for aviation security.

B. THE AIRPORT OPERATOR'S ROLE

Maintaining a transportation environment that is safe from sabotage or acts of terrorism is perhaps the most crucial duty of the airport operator. An airport operator juggles many roles and has numerous responsibilities, which are outlined in federal regulations that are essential to safety and security. One of these responsibilities, outlined in 49 CFR 1542.201 (4), is to mandate specific criteria to allow employees unescorted access to the secure areas of the airport.

Airports typically adopt a multi-pronged approach in an effort to minimize the danger to aviation that is presented by the insider threat. The most notable emphasis has been in physical-security requirements. These physical-security requirements include guarded entrances, closed circuit television (CCTV), biometric devices (to ensure identity at the entrance), and random police patrol. Unfortunately, due to the resourcefulness of the employee insider, these physical-security barriers are easy to navigate and decipher once the insider is embedded behind the scenes in the work place.

C. FEDERAL REGULATIONS AND AGENCIES

Airports and airlines are regulated by an array of federal agencies. These agencies include, but are not limited to, the Federal Aviation Administration FAA), Customs and Border Protection (CBP) and the Transportation Security Administration (TSA). Federal regulation 49 CFR 1542.209 requires employees that work at airports and have access to restricted areas are required to meet certain specific requirements for criminal history and pass background checks. Once they have completed this process, they are issued airport identification media (badges) to allow them access to restricted areas. A number of issues remain that are open to exploitation by perpetrators.

- Employees can receive a badge once found to be free of disqualifying crimes at the time of the badge application. There could be other less significant crimes that may not disqualify an employee but could demonstrate a pattern of behaviors that may lead to more severe crimes at a later time.
- Employees may not have any crimes at the time of application but may commit crimes after they receive their badge. The crime may be one that would disqualify an employee from receiving a badge. However, since the employee has already received a badge, and not required to go back through the background process, he/she may not be identified through the current system.
- An employee may not have any disqualifying criminal convictions but could be corrupted by bribery or extortion to aid an individual or organization intent on doing harm to an aircraft.

D. CONCERNS, CONSEQUENCES, AND COUNTERMEASURES

The consequences of these vulnerabilities could be devastating. An employee could simply carry a weapon into the restricted area and provide an individual or groups of perpetrators with weapons on the secure side of the airport after they have been processed by TSA passenger screeners. Once inside the secure area, the armed perpetrators would have no additional security scrutiny prior to boarding an aircraft. Other means of sabotage could also occur such as placing explosives on aircraft in the cargo holds, damaging flight control or propulsion systems, or secreting other individuals through employee portals undetected.

Congress, the media, and other groups have expressed concern at the current system. One solution proposed by individuals within congress is 100 percent employee screening.2 Individual Congressmen have threatened 100 percent employee screening as a mandated and regulated solution to the dilemma. In some cases, a pilot program for 100 percent employee screening was conducted at several U.S. airports (U.S. House of Representatives, 2007). It is generally agreed among aviation security professionals; this

[2] One hundred percent employee screening in the context of this problem statement is defined by the Congressional Committee on Homeland Security in a report directing the Assistant Security of DHS to address vulnerabilities in aviation security by carrying out a pilot program to screen airport workers. In this report 100 percent employee screening is described as application "of the same standards as apply to passengers at airport security screening checkpoints."

is not a practical or realistic solution. The cost of such a solution would be extraordinary and in some cases put commercial airlines out of business. Likewise, the notion that airports could realistically screen their entire population of employees with over 100 percent effectiveness over the course of the working day is naive at best. Any fixed system, process, or procedure, such as 100 percent employee screening, will just be another measure that the insider will learn to manipulate. Once employees learn the process, those that would inflict harm will learn ways to defeat the screening process.

Airports and other critical infrastructure that have miles of secure perimeter to protect, all have similar vulnerabilities. If an employee is required to go through a screening checkpoint as he/she arrives at work, there is not a measure in place or currently feasible to deny an insider from driving or walking to a remote location on the secure perimeter and passing weapons or other dangerous items over, under, or through the perimeter fence. The screening of 100 percent of the employees only determines if they have authorization to be in the restricted area, and if they are free of weapons, explosive devices, or prohibited items at the point they are screened. A multitude of other opportunities to acquire contraband are available to an insider following screening.

Aviation security experts widely agree the proposed solution (100 percent employee screening) falls short of addressing the problem in a manner that would reduce the threat in such a way that would justify the expense (Government Accounting Office [GAO], 2009). There is not a system that is capable of determining whether they are friend or foe.

E. RESEARCH QUESTIONS

In order to determine a course of action going forward, a central research question was developed. The central research question stated simply was:

- What measures can be implemented to disrupt threats from insiders to commercial aviation?

In order to more fully inform the research, a series of sub-questions were developed to focus on what methods are currently being applied to the problem, what methods are being proposed, and what measures can be applied or enhanced to further address the problem. The sub-questions were as follows:

- How is the insider threat managed, and what are their strengths and weaknesses?
- What methods of managing the insider threat are being proposed and what are their strengths and weaknesses?
- How can current methods be further enhanced to strengthen commercial aviation against the insider threat?

F. ARGUMENT

The insider threat presents a significant threat to commercial aviation security. A person on the inside is a subject matter expert in his area of operations as well as having an above average knowledge of the workings of the airport and its security.

Given that insiders are quick to learn how to work any system that may be put into place, it seems that a more sophisticated approach is in order. For an approach to be effective in detecting and deterring an insider, it should be a dynamic system that is based on varying levels of security in a layered fashion, executed in a random manner (Elias, 2009).

The focus of this research will be to develop recommendations to policy makers on enhanced and alternative methods to identify employees and behaviors that may present a threat to aviation security. The recommendations will be derived from a review of existing procedures employed for vetting airport employees. In addition, enhanced and alterative measures not currently employed in the aviation environment will be evaluated to consider their value in further security the integrity of the restricted area.

G. SIGNIFICANCE AND SUMMARY

The threat posed by aviation insiders is a highly complex problem. It is unlikely that U.S. aviation will ever be able to eliminate the threat posed by aviation insiders;

however, measures can be taken in the short term to improve the resistance of the current aviation environment to the threat. This thesis explores the vulnerabilities with the current system and makes recommendations to close the gap posed by nefarious aviation insiders.

This thesis will allow policy makers to view the problem presented in a comprehensive yet uncomplicated manner. It will allow policy makers the opportunity to understand the problem, its magnitude and its potential consequences. More importantly, this thesis lays out a pathway to significantly reduce the vulnerability to aviation presented by aviation insiders.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

Aviation security and the betrayal threat presented by insiders received attention following September 11, 2001; however, it has been a concern prior to those attacks. Government officials called for security increases addressing the insider threat before the attacks of 9/11 (Miller & Dover, 1998). Following the attacks of September 11, the 9/11 Commission specifically recommended the Transportation Security Administration develop a plan that included enemy tactics such as insider threat in its final report (National Commission on Terrorist Attacks upon the United States [9/11 Commission], 2004).

Detection and deterrence of the insider threat in aviation continues to evolve as a regulatory matter. The U.S. government, specifically the TSA has been charged by Congress to execute laws created by legislative means to hold airports and airlines accountable for the behavior of rouge employees.

While aviation security has been a topic of discussion for many years, the events of 9/11 moved aviation security to center stage. U.S. airports remain at an elevated level of security. This heightened level of security, level orange, is one level above the rest of the United States, currently at level yellow. Recently, the discussion brought to the forefront of the debate by many aviation experts, congress and concerned citizens, is the issue of insider threat. This is the result of the widely publicized arrest of individuals working in the aviation industry for charges ranging from theft; to the smuggling of guns, drugs, cash, and illegal aliens in commercial aircraft (GAO, 2009). Congress, the public, and aviation experts recognize the opportunity these criminal networks and activities pose to those that would seek to perform acts of terrorism in aviation.

Volumes of literature have been published that suggest the threat to aviation security by the insider threat is a possibility. Congress, aviation experts, the media, and the traveling public all agree the threat to aviation security presented by employees who have unescorted access to sterile areas of airports, present vulnerabilities. The

recognition of the vulnerability was evidenced in literature from congressional testimony, Government Accountability Office (GAO) reports, professional trade journals and "for official use only" reports.

A review of the available literature on the matter of aviation insider threat was conducted. Generally, some literature was available on the topic but by in large it was confined to a few areas. Those areas were:

- Is the threat from aviation insiders legitimate?
- What is the national strategy on aviation security?
- How do the federal regulations address aviation security and the insider threat?
- Who are the "insiders"?
- What methods to manage the insider threat are being written about?

A. IS THERE A THREAT FROM AVIATION INSIDERS?

Literature is available that highlighted the vulnerability to aviation by the threat posed by insiders. The literature is presented in reports regarding criminal activity by aviation employees. This literature is relevant in legitimizing the insider threat as a valid method of perpetuating violence against commercial aviation. In light of the absence of a large number of more relevant examples of insider activities of this nature, the literature demonstrates the vulnerability exists, despite the fact that it has not been used to perpetuate a terrorist attack.

As recently as September 2009, Najibullah Zazi, a 24-year-old Afghan immigrant and former Denver airport shuttle-van driver, was arrested on federal terrorism conspiracy charges (Bliss & Blum, 2009).

One recent report regarding fraudulent acquisition of security badges by illegal immigrants, highlighted vulnerability in determining employee identity (12 Charged, 2009). The report outlined a sting at a New York airport where 12 employees were charged with using forged immigration documents to verify their identity and thus

acquire airport security badges (12 Charged, 2009). While this does not constitute a terrorist ring, it does demonstrate the ability for individuals to be granted access to secure areas under the pretense of legitimate means.

Another similar incident occurred at Chicago's O'Hare Airport where the owner of a temporary employment agency was sentenced in October 2009 to three years in prison (Chicago Tribune, 2009). The owner had manufactured dozens of fake security badges for her mostly illegally immigrated staff, allowing them to perform duties in the secure area of the airport. Here again, this fraud was perpetrated not for the intent of a terrorist attack but to enable workers that would otherwise not qualify for a legitimate security badge due to immigration status, to work in the restricted area of the airport. Nevertheless, the nexus to terrorism utilizing the same method of operation was emphasized by the local news agency.

In 2008, an elevator mechanic was arrested for smuggling at least 17 illegal immigrants including two with criminal records. He is suspected of being part of a larger smuggling ring that used him to gain access to restricted areas at Los Angeles Airport (LAX) (Wikel, 2008).

In:

> …June, 2007, four individuals were charged with conspiring to attack JFK Airport by planting explosives to blow up the airport's major jet-fuel tanks and pipeline. The plot aimed at detonating the fuel tanks, resulting in exploding fuel pipes running underneath passenger terminals. The four individuals including a former JFK cargo worker, Justin DeFreitas were arrested. DeFreitas was dispatched to conduct surveillance on the pipeline starting in January 2007. DeFreitas used his knowledge of air and ground operations at the airport to survey possible targets. (Collins, 2010)

The nexus to terrorism in these cases is limited; however, the ability for a malicious insider with a desire to inflict violence through their unescorted access to secure areas is obvious.

B. NATIONAL STRATEGIES

The *National Strategy for Aviation Security* (NSAS) was published in March, 2007 (White House). The broad strategic plan does not specifically address the threat to aviation from insider attack. However, it does acknowledge, in broad terms, that "the Department of Homeland Security is responsible for coordinating the overall national effort to enhance the protection of critical infrastructure" (White House, 2007, p. 13). It continues by indicating the major areas of national security to include, "…investing in protective measures such as staff identification and credentialing, access control, and physical security of fixed sites" (White House, 2007, p. 13).

The *Aviation Transportation System Security Plan* (ATSSP) intended to support the NSAS was published on the same (2007). This plan provides additional granularity to the *National Strategy* by developing and implementing measures to reduce vulnerabilities within the aviation transportation system. The ATSSP outlines three critical system areas to further reduce vulnerabilities. One of the three critical system areas it mentions is to "ensure that anyone entering or using the aviation transportation system has been identified and vetted or screened" (Aviation Transportation, 2007, p. 1). It elaborates on this area by indicating a direction to explore access controls, adding biometric identifiers to employee credentials as well as enhancing physical security programs to apply to all airport employees and vendors.

C. FEDERAL REGULATIONS

Prior to September 11, 2001, the regulatory authority for aviation security was held by the FAA. A final rulemaking change was made in February, 2002 that assigned this authority to the newly created TSA (Department of Transportation [DOT], 2002). Regulations found in the Code of Federal Regulations (CFR) at 49 CFR Parts 1500, mandate the various aspects of aviation security shared by the TSA, the airport operator, and the aircraft operator. The regulations are very broad in the various aspects of aviation security such as passenger screening, law enforcement responsibilities, airport security program, and operations to name a few. The areas of particular relevance for this literature review are confined to the topic of insider threat. While the term insider

threat is absent from the regulation, the rules and regulations include the various aspects of identifying, eligibility, credentialing, and training of airport workers.

D. WHO ARE THE INSIDER THREATS?

Limited literature is available to assist security experts in developing profiles of individuals that have exhibited malicious insider attacks in advance of violent action. One such source was an article entitled, "Refining Insider Threat Profiles" (Kirkpatrick, 2008). This article was focused on the broader context of insider threat beyond aviation. This included information systems and financial institutions. The author, Kirkpatrick, provided a categorization of insider motivations to include disgruntled employees, insider threats brought on by nationalistic reasons, greed motivations, as well as ideology. The article concluded with offering that raising awareness of the numerous types of insider threats among practitioners and researchers can help to advance the understanding of new indicators that may assist in identifying threats in advance of attack (Kirkpatrick, 2008). The article fell short of providing any concrete actions that security practitioners could employ to manage the insider threat. Generally, it indicated a need for additional research in the subject area.

The first written evidence I was able to find during the literature review of specific aviation awareness of the insider threat, was unclassified/for official use only (U/FOUO) reports beginning in 2007. The DHS and the Federal Bureau of Investigation (FBI) published a Joint Homeland Security Assessment in August 2007 (Office of Intelligence and Analysis and Federal Bureau of Investigation, 2007). This four-page U/FOUO report revealed three key findings that summarized three plots to attack U.S. interests.

In April 2008, the TSA published a U/FOUO information bulletin titled, "Clean Skins, Lone Wolves, and Insiders" (Transportation Intelligence Gazette [TIG], 2008). This four-page report provided definitions and examples of the three actors referred to in the report as Clean Skins, Lone Wolves, and Insiders (TSA/TIG 2008). The bulletin was useful in continuing to raise awareness of the existence of violent actors but failed to provide any guidance to the end user on how to detect or manage the insider threat.

In February 2009, the TSA's Office of Intelligence published a U/FOUO bulletin (TSA/Office of Intelligence [TSA/OIS], 2009). Here again, this bulletin was useful for raising awareness among security practitioners regarding the potential for threats to emerge from within the aviation industry. The bulletin described plots and actors that had participated in planning for attacks (TSA/OIS, 2009). In some cases, these examples were republished from the 2007 and 2008 reports. No suggested actions were included in this report as to how to detect or manage insider threats.

E. METHODS TO MANAGE THE THREAT

A number of methods to manage the threat were documented. Those methods included the development of a previously discussed threat profile, 100 percent employee screening, managing insider threats using threat assessment methods, technological solutions such as biometric systems, surveillance, and tracking.

One hundred percent employee screening, the physical screening of employees prior to entering secure areas, has been proposed as one the solutions to mitigate the threat posed to aviation by the insider. Some members of the U.S. Congress have been vocal and supportive in this regard (TSA, 2008). Opinions vary on the practicality and feasibility of screening employees prior to having access to secure airport areas.

Managing insider threats using threat assessments is documented in one aviation management journal (Randazzo, 2008). This journal article provides a list of warning signs that allow aviation security managers to monitor what might be precursors to violent activity perpetrated by an insider (Randazzo, 2008). In addition, the article provides a step-by-step method to create and develop threat assessment capacity (Randazzo, 2008). While this is useful in detecting and managing the threats from traditional insiders, those who seek revenge against a company or who are otherwise disgruntled, it does not recognize the threat from a non-traditional actor such as an ideologically motivated insider actor.

Another area addressing insider threat management methods are those derived from technological solutions. A diverse array of technological solutions such as biometric systems, surveillance, and tracking are on the market and well documented.

While many private manufacturers provide compelling and sophisticated use of technology to monitor the movement of employees and to insure proper identification of employees, professionals should be suspicious of salesman that may have financial reasons to make the reader believe their product provides the highest degree of protection from the insider threat.

The literatures published by the Government Accountability Office (GAO) are the most comprehensive in terms of the insider threat to aviation. Despite the fact they are comprehensive, the GAO reports to Congress (GAO, 2004; GAO 2009) focus on the fact that insider threat is a potential security issue and 100 percent employee screening is expensive and an ineffective approach. With the focus of the GAO reports being on recognition of the threat and reviewing only a single method of mitigating the threat, they were not particularly useful in evaluating other enhancements that would diminish the threat to commercial aviation. GAO reports, as well as the other literature included in this review, are absent any strong direction, regulatory or voluntarily to provide a consistent, innovative management approach or plan addressing the vulnerability presented by the insider threat.

In reviewing the literature, it appears that government officials, federal and local, are unable to see past the prescriptive elements of physical security. In order to be more effective at identify employees that would desire to do intentional harm to aviation; a more comprehensive approach would present a more reliable outcome. A comprehensive approach that includes a more thorough and perpetual vetting of employee's background, including physical security measures, would yield the most likely positive outcome. It should also, be understood that no measure will completely eliminate the threat. Waiting for the perfect solution impedes progress and should not be used as an excuse to do nothing.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. METHODOLOGY

A policy analysis methodology will be applied to this thesis. This methodology is appropriate to answer the research questions, as policies are currently in places that are, in part, set in place to disrupt threats from aviation insiders. In order to recommend enhancements or a change in direction, it would be critical to fully understand the policies in place. Once clarity in understanding what the policies were intended to address, it would be beneficial to the research to analyze the results of the measures to determine if the policies were effective, or if they needed to be rewritten or strengthened through amendments to the existing policies. The policy analysis would allow for the exposure of policy strengths and weakness.

Federal regulations, specifically 49 Code of Federal Regulations (CFR) 1542 and 49 CFR 1544, mandate requirements for airport operators, commercial airline companies, concession companies as well as individuals that apply for and/or receive security credentials to allow employees to access secure areas within the airport environment. This thesis will provide an analysis of the existing federal requirements, under 49 CFR 1542 and 1544, and recommend modifications to the requirements to further strengthen the current policies and practices.

B. SAMPLE

Sample data was collected during a review of records at the Dallas-Fort Worth International Airport (DFW). While minimum requirements for the identification and checking of employee history, through criminal history records checks, security threat assessments and employee name comparisons against the “no-fly” list and other “watch lists” are provided within the policy, DFW Airport exceeds the requirements in certain areas. Although DFW Airport represents a single source of data, it is the third busiest

airport in the world and has a large employee population (approximately 30,000).[3] Data was provided by DFW Airport, including employee data, which served to provide a large sample of how some measures might influence an airport's ability to reduce potential threats from unscrupulous employees.

Beginning in 2007, DFW Airport began to randomly submit 15 percent of all badge renewals for a criminal history records check.[4] As a result of this new procedure, over the minimum requirements of the policy, data accumulated over the three-year period is available to analyze the effectiveness of the new enhanced procedure or the in-effectiveness of the existing policy. In addition, the data would be helpful in determining if a higher number of badge renewals should be subjected to the same criteria as a minimum requirement. This data will also demonstrate the effectiveness of the policy that requires employees convicted of one of the policies' 28 disqualifying crimes and must self-report the conviction was effective. The number of employees discovered to have convictions disqualifying them from badge renewal would serve to verify the hypothesis that employees have no compelling reason to self-report convictions. Therefore, the analysis will consider other options to compel an employee to report the conviction.

In addition, CBP has an additional step beyond DFW Airport's employee vetting in order to allow access to the Federal Inspection Station (FIS).[5] In some cases, while an employee may pass the requirements to receive an airport badge, he or she may fail the requirements of CBP's more restrictive process and not be allowed FIS access. The reason why CBP would not approve an employee to work in the FIS is privileged information and not readily available to the airport operator. However, the rejection by CBP does not restrict the employee's ability to work in secure areas not within the FIS. This fact should give airport operators pause.

[3] Information obtained by author through databases with DFW Airport not available to the public.

[4] Ibid.

[5] The Federal Inspection Station (FIS) is the location where Customs and Border Protection receives and processes passengers at international airports that are arriving into the U.S. from foreign countries.

Understanding this percentage of employees that fail this additional step would provide a glimpse of a larger problem. These percentages experienced at DFW Airport would also be of value in determining the breath of the problem within the national aviation system. In addition, an opportunity to review existing procedures, which appear to be redundant, could provide a more robust picture of employee behaviors.

Federal regulations govern all U.S. airports. Therefore, all airports in the United States use a similar method to manage the threat presented by employees. It is helpful to look beyond our nation's borders to evaluate best practices at foreign airports in an effort to determine if their practices might have an application to the domestic aviation domain. For the purposes of benchmarking against other international airports, large Canadian airports were selected. For this analysis, data was provided by the airports in Montreal and Toronto (Canada).

These airports were selected for a number of reasons. First, it was important to find airports with a track record of success in the management of insider threats. Reviewing airports with documented failures would damage the creditability of the analysis. Secondly, it was imperative to determine if the airport had a high potential for insider threat and, thus, a realistic expectation that practices employed at the airport were necessary and effective.

Next, the airports needed to be in a country with a similar free society. Airports in communist or dictatorial societies have methods of dealing with employees that would not be easily applicable to the United States. Finally, the airport must be one that would share information on their practices openly. In these cases, a long and well-developed relationship among aviation security professionals is in place that allows for some sharing of sensitive information.

Canadian airports use a methodology similar to the United States in vetting airport employees through the mandates of federal regulations. There are significant differences in who performs the background checks and how the information is shared. Some of the data that would be useful to this thesis is unavailable, since it is considered security

sensitive; however, the regulations are accessible and easily available allowing for comparative analysis between U.S. regulations and those of the Canadian government.

C. DATA COLLECTION

Data was collected by the author from the database at DFW Airport's Access Control Office (ACO). The ACO is the office having primary administrative responsibility for the collection, processing and issuance of airport identification security media (badge). This is a highly complex process that integrates the identification of employees, fingerprinting and capturing of other relevant and required data. Once captured, the ACO transmits the data to a clearinghouse where employee vetting occurs across multiple federal agencies. One result of this step in the process is the return of criminal history derived from federal records. This criminal history is checked for disqualifying crimes and a badge is issued or denied based in part on these results. This data, while not normally complied in a format useful to this research, was assembled for a 45-month period (January 2007 to September 2010).

With regard to the Canadian regulations, the policies were available on the internet. The regulations were downloaded and analyzed.

D. DATA ANALYSIS

Airports and airlines are required to run criminal history records checks on new employees prior to issuing a security badge; however, regulations do not require additional checks later in the employee's career even though a security badge is typically renewed every two years. DFW Airport has a practice of checking 15 percent of the employees renewing applications each year. This random process provides DFW Airport, as a representative sample, the ability to demonstrate patterns of employees that have failed to meet their regulatory obligation to self-report convictions. As such, this data can be presumptively extrapolated across the U.S. aviation system. Analyzing the increase or decrease in the percentage of employees that failed to be approved for badge renewal yields an estimate of the value of these additional steps to national aviation security

In addition, employees that desire access to the U.S. Customs and Border Protection Areas, within an international airport, are required to undergo additional background checks by CBP. There are occasions whereby employees will pass the criminal history records check conducted by airport/airline institutions but will be denied access to the CBP areas due to irregularities within the employee's background that cause CBP to deny this privilege. In these cases, the employee retains his/her badge but is assigned duties at the airport, in other secure areas but not allowed access to CBP areas.

The method of research began with a comprehensive review of the regulations that govern the management of aviation employees both physically and non-physically. Physical measures, for the purpose of this research, are considered to be barriers, fencing, CCTV, and others that are designed to fortify an aviation perimeter, terminal building, or other support buildings, thereby denying unauthorized or unintended access to persons, including employees. Non-physical measures are considered background checks, including security threat assessments, criminal history records checks, credit checks, and personal references that are designed to paint a picture of an individual's future behavior based on past behaviors. During this phase of the analysis, it became clear that physical measures, while an important component in the management of insider threats, the reality is that any measure taken to restrict entry, movement or access, could be defeated in complex venues such as an international airport.

The next step in the research was a review of available literature, beyond regulations, to determine what methods had been implemented or tested and how the new methods had performed, and if additional methods were being considered for implementation or testing. Based primarily on the available literature, additional physical measures were generally characterized as costly and easily defeated by industrious employees. Therefore, the research began to focus on measures on the non-physical track. The purpose was to determine if other measures to enhance existing non-physical measures or if new dimensions of non-physical measures could be added and thereby improve the current situation.

In order to provide some measurement of the expected success of recommendations to increase the effectiveness of the policies under review, criteria for

judging the recommendations was necessary. A matrix was created that includes the effectiveness, public perception, the implementation cost, and the ease of implementing the recommendations.

The effectiveness of the recommendations was determined by predicting the number of employees that are discovered to have convictions for crimes that disqualify them from retaining airport security credentials. This dimension may not be immediately recognizable until the recommendations are implemented; however, there is quantitative evidence from at least one major airport that provides data on the number of employees that have been convicted of a disqualifying crime following receipt of a badge.

Public perception regarding aviation security is an important driver of many of the security activities performed at airports. Currently, the average consumer of the airport is no doubt unaware of vulnerabilities within the current systems and methods used to verify employee identity and in managing the threat potential from this group over the course of what could be a two or three decade career.

Any action or method proposed by this thesis will impact the employee base, not necessarily the public-at-large. Other measures have been implemented since September 11, 2001 that are specifically designed to validate employee identity and criminal history. While those measures are believed to fall short of a comprehensive review of employee behaviors, a review of the reaction from the public to those measures from the past are believed to be replicated in any new measures proposed in the future.

The implementation cost criteria can be ascertained with some degree of accuracy. The logistics of such enhancements are believed to be fairly easy to identify. Costs for recommendations will be applied to a cost-per-enplaned passenger matrix that will demonstrate the anticipated percentage of cost against the cost airlines/airports typical calculate to drive ticket prices.

The ease of implementing the recommendations was judged based on variables to include push back that might be expected from the public and congress.

Table 1. Matrix

Effectiveness	**Public Perception**	**Implementation Cost**	**Implementation Ease**
Low—High	Favorable—Unfavorable	Low—High	Easy—Difficult

THIS PAGE INTENTIONALLY LEFT BLANK

IV. ANALYSIS/FINDINGS

The findings from this study provide important insights for understanding of a complex set of security gaps associated with mitigating the aviation insider threat. These findings lead toward the development of a set of recommendations that are collated into an easily understandable and non-distracting set of holistic changes designed to work within an emergent threat in a highly complex airport security environment to mitigate the insider threat and enhance security at U.S. airports.

The analysis is organized in four sections. The sections are designed to uncover underlying structures and processes and to demystify and clarify the current issues facing aviation security professionals, which will allow for a more focused understanding of the current degree of vulnerability and what actions should/can be taken to close the vulnerabilities.

This chapter will first analyze 49 CFR 1542 and 49 CFR 1544, which are the federal regulations that specifically provide authority for the state, local, and private sector to address the insider threat. In addition, it will outline the commonly applied concepts that airport and aircraft operators utilize in their attempts to satisfy the requirements of the regulations and more specifically to disrupt threats from aviation insiders.

Next, this chapter will analyze a popular strategy that is believed to enhance the management of threats from aviation insiders by screening the aviation employees using the methods normally considered in screening passengers. Finally, this chapter will identify and analyze enhancements to the current methods of managing aviation insider threats, as well as concepts of background checks that are common in other venues. Those concepts include, but are not limited to, employee behaviors such as: criminal, financial, and employment history.

A. THE CURRENT MODEL FOR THE MANAGEMENT OF AVIATION INSIDER THREATS AND LOCAL APPLICATIONS

The 49 CFR 1542, Airport Security, addresses the airport operator's role in securing aviation. Within 49 CFR 1542, this research focused on sections, 1542.201, "Security of the secured area", 1542.205, "Security of the security identification display area (SIDA)", and 1542.209, "Fingerprint-based criminal history records checks (CHRC)". These sections are directly linked to employee related matters, such as background checks, that have bearing on insider threats. These sections were analyzed by evaluating their strengths in four areas outlined in a matrix (see table 1). Those areas included the overall effectiveness of the federal requirements to address the threat to aviation presented by insiders, the perception of an interested public as to the appropriateness of the measure, the cost to implement changes to the regulations, and the ease in implementing changes to the regulations.

The 49 CFR 1544, Aircraft Operator Security: Air Carriers and Commercial Operators, addresses the air carriers and aircraft operator's role in securing aviation. Within 49 CFR 1544, sections 1544.201, "Acceptance and screening of individuals and accessible property", 1544.225, "Security of aircraft and facilities", 1544.229, "Fingerprint-based criminal history records checks (CHRC): Unescorted access authority, authority to perform screening functions, and authority to perform checked baggage or cargo functions", 1544.230, "Fingerprint-based criminal history records checks (CHRC): Flight crew members" were also analyzed and mapped against the insider threat matrix.

Currently, the threat from attack by an aviation insider is managed by various stakeholders that include federal, state, and local officials. Likewise, private sector having employees working in secure areas also have a stake in the management of the insider threat. Although various stakeholders have an interest, the primary portion of this shared responsibility lies with the airport operator.

Airport operators have primary responsibility for the physical security of the secure areas of the airport. Typically, airport operators deploy physical measures that are utilized to deny entry to secure areas of the airport by those not authorized to enter.

Those physical measures take the form of gates, fences, locks, and other traditional security devices. In addition, airport operators typically hire security officers to maintain the integrity of security at certain points where more positive control and identification are necessary. Airport operators are also the primary entity that issues airport identification to employees authorizing access to the secure areas.

B. THE BADGING PROCESS

Assuming employees have authorization to enter the secure areas through the physical measures: the first line of defense to managing aviation insiders is through the issuances of airport identification (badge) to employees to allow access. While the badge is a visible, outward symbol allowing for immediate recognition of an employee's authority to enter secure areas of the airport, the real value of the badge lies behind what is not outwardly visible. This value is in the badge application process that leads up to the issuance of the badge.

The badging process is a highly regulated (49 CFR 1542. 209), complicated, multi-step process that can become protracted. It begins with an authority, the badge sponsor, who is generally the employer who must sign a document verifying that the employee is in need of a badge. The next step is for the employee to verify his identity that he is in fact, the person who is being sponsored for the badge. This verification requires two forms of identification, including at least one photo ID.

Following verification of identity, fingerprints are captured for the purpose of completing a fingerprint based criminal history records check (CHRC). Airport operators, under 49 CFR 1542.209, have the authority and the requirement to conduct a CHRC. Aircraft operators are permitted this same authority and are required, to conduct a CHRC under the 49 CFR 1544.229.

Employees or applicants that have a criminal history for one of 28 disqualifying crimes (49 CFR 1542. 209d) are automatically disqualified from the ability to have unescorted access to secure airport areas by virtue of not being issued the requisite badge (see appendix A). In addition, a security threat assessment (STA) is completed on each employee by the federal government. The exact steps within the STA are classified, but

it is well known that names of individual employees are checked against a range of federally managed lists. Having employee's names on one of these lists, such as the "No-Fly list", is sufficient for a denial of the employee for badging until such time as the issue is resolved. Once all the steps are complete, in approximately two to three weeks, the badge is presented to the employee.

C. STRENGTHS BUILT INTO THE PROCESS

The badging program has some significant strengths that makes this method of management of the insider threat a viable tactic. First and foremost, the badging process places strong emphasis on determining and verifying the identity of the individuals presenting for a badge. This is a linchpin step, which without the confidence that a person applying for the badge is legitimate, would make the remaining steps ineffective. Two forms of identification, one government issued and one including a photo, provides a heightened degree of confidence that the subject presenting for a badge is, in fact, the person who is pictured in the ID.

Second to positive identification of a subject, the finger-print based criminal history records check (CHRC) is the most valuable step. This strength is founded in two aspects. One positive attribute of the CHRC is that is adds additional vetting of the employee's identity. Certainly, having a fingerprint to further identify an individual is the panacea of identification verification. The other positive attribute of the CHRC is the ability to review the individual's past criminal history for both disqualifying crimes, as mentioned earlier, or for patterns of criminal misbehavior. These patterns of behaviors may or may not indicate a pattern of behaviors rising to the level of disqualifying offenses, but may demonstrate a threat to aviation cumulatively.

The third strength to the current badging process is the security threat assessment. The STA is purportedly completed on a perpetual basis. In other words, the names of employees that are being issued a badge, or that are in possession of a badge, are checked in real time in an active way. A variety of federally managed lists containing names of known or suspected terrorist or criminals are pinged perpetually. If an employee's name

appears on one of these lists, it allows law enforcement personnel to take proactive action to detain/arrest or otherwise remove the threat from the secure aviation environment.

D. WEAKNESS IN THE PROCESS

Unfortunately, the badging process is not without its shortcomings or weaknesses. One such weakness lies in the ability to verify a person's Identity with 100 percent confidence. Forms of identification are required by federal statue in order to prove identity and to begin the badging process. As there is no single, universal form of identity, federal guidance specifics what forms of identification are acceptable to prove identity and to establish authority for an individual to be employed. This guidance is attached to this report (see Appendix B).

In some cases, certain forms of identification can serve to both positively identify the individual and as proof of employment status. Such documents include a U.S. passport or other forms of alien registration cards. An alternative for those that do not have a passport or other alien registration authority is that they are required to produce two forms of identification. Most commonly, U.S. citizens will present a drivers license or ID card and a social security card. Other acceptable forms of identification include a school ID card with photograph or a voter registration card. Approved identification must be issued by a government authority, and one of the identifications must have a photo of the individual. This level of identification for access to areas of security in the airport environment are easily reproduced and thus an area of concern.

Fingerprints were highlighted earlier in this chapter as being highly reliable as a form of identification. Naturally, for this step to add this value, the individual's fingerprint must be on file with law enforcement to match the individual with the fingerprint. This is not always the case, and as such, fingerprint identification has it limits.

Fingerprint-based CHRC also adds value by determining the past criminal history of an employee. While criminal history cannot predict the future, past behaviors provide a measurement of an individual's ability to abide by the law; however, this step is only of

value if the individual has been arrested or otherwise has a criminal history. It is not safe to assume that an individual is not a criminal or terrorist risk to aviation based on the absence of a criminal history.

Individuals convicted of one of the disqualifying crimes, in the past 10 years, are automatically denied a badge; however, an automatic denial is only relevant for convictions. Criminal history that indicates a prior arrest for acts of terrorism, absent a conviction, on its own merit, would not automatically create a denial for a badge. In this case, a review would be conducted by the appropriate authority to determine if other mitigating circumstances could either allow a badge to be provided to the individual or with-held.

In addition, there is the possibility that an individual, having only lived in the U.S. for a short period or other country that law enforcement does not have a good criminal information sharing network, might apply for a badge. For example, an individual, who has recently immigrated to the U.S. from a country that has known ties to terrorist organizations, could apply for a badge. In this case, it is unlikely that U.S. law enforcement would be able to, with any confidence, gather criminal history information from an unfriendly country. This inability to look back with confidence at an individual's criminal patterns presents a significant blind spot for decision makers responsible for issuing badges.

One additional weakness associated with the CHRC is the split responsibility of the decision-making process between the airport operator and the aircraft operator. As previously stated, all applicants are required to undergo a thorough CHRC when they apply for airport identification.

In addition to specifying the crimes that would disqualify an applicant from receiving a badge, Federal Regulation 49 CFR 1542.209(n) also allows the airport operator to not grant a badge based on other mitigating circumstances. For example, the list of disqualifying crimes does not include possession of a controlled substance; however, an airport operator can deny access to an applicant with a possession charge on their CHRC. The operator is authorized to use his/her judgment to deny the badge if he

or she has concerns that the applicant's past history could negatively impact airport security. In these border-line cases, an airport operator may interview the employee to gain additional knowledge about his or her past and then make a decision based on the merits of the interview. At one U.S. airport, Dallas Fort Worth International Airport, this decision making and interview process is carried out by a trained police detective.

Aircraft operators that hire under 49 CFR 1544 (air carriers) are given the same opportunity to accept or reject applicants based on criminal history or other mitigating circumstances. However, it presents numerous conflicts of interest for private companies to have the ability to override security practices that might conflict with their business interests. Recall that U.S. Congress removed the responsibility from private airlines to perform passenger screenings following the tragic events of September 11, 2001. This should cause one to pause and ask if this might be a conflict of interest.

The airline/private sector is responsible for conducting the criminal history screenings for over 15,000 of the 28,750 badged employees at DFW.[6] This is a significant percentage of the entire employee base. It should be noted that at no time does a trained police detective, as an agent of the airport operator, have the opportunity to review the airline employee's CHRC.

Another significant weakness of the badging process is the absence of follow through after the issuance of a badge. Typically, badges are considered valid for a two-year period. Once the badge expires, the employee is required to resubmit for a badge renewal.

There is no federal requirement to verify that during the period an employee is badged, he/she has not committed and been convicted of additional crimes. There is a requirement, 49 CFR 1542.209(e), for employees to self-report convictions of any of the disqualifying criminal offenses within 24 hours of the conviction. This requirement is unrealistic considering that employees reporting a conviction of one of the disqualifying crimes would lose their privilege to have a badge or unescorted access and would most likely have their employment terminated. There is very little, if any, incentive for an

[6] Information obtained by author through databases with DFW Airport not available to the public.

employee to report a conviction of a disqualifying criminal offense or any other crimes that might be useful to the airport operator/aircraft operator in being able to connect the dots on employee behavior and the potential for an insider threat.

The fact that some employees will be convicted of crimes following the issuances of a badge should not be a question. The question might be how large of a problem is this reality. Anecdotal data was collected from one major airport. During a three year period (fiscal year 2007–2009), DFW Airport checked CHRC for employees that renewed badges. The CHRC was limited to only 15 percent of all the badges that were expired and requesting renewal. Therefore, of the 24,364 incumbent employees that requested a badge to be renewed; only 6,777 were submitted for an updated CHRC.[7] Of the 6,777 incumbent employees submitted from CHRC, six (one percent) were disqualified from badge renewal based on the results of the CHRC. Applying that same data across the total of employees requesting a badge renewal, another 16 employees would have been disqualified. While this percentage of employees, when characterized in percentages may appear to be low, the fact that 16 employees could continue to possess badges, and thus access to the secure aviation areas of the airport, is disconcerting.

It is also important to remember that the only other method currently in place to identify an employee with a conviction subsequent to employment is through the employee self-reporting the conviction. Equally concerning is the fact that an arrest for one of the criminal offenses or any other offense would not create a requirement to self-report, only a conviction. This is discussed in more detail later in this thesis.

Some might contend that the STA, conducted on a perpetual basis, is a back stop to such behavior that might signal officials to the presence of a criminal offense. However, as recently demonstrated with the Christmas Day attack on aviation in Detroit (2009), this assessment is a valuable tool but has weaknesses within its applications. Furthermore, criminal offenses on their own would not necessarily cause an individual's name to be added to any of the various lists designed to target potential terrorist.

[7] Information obtained by author through databases with DFW Airport not available to the public.

Moreover, the finger print based criminal history portion of the badging process is limited to criminal behaviors only. Other common behaviors are frequently included in background investigations. Background investigations frequently include aspects of a person's behavior that might, on their own, not indicate a propensity to be a threat to aviation but when looked at as a piece of the whole, might raise suspicion with a trained investigator. Those other elements could include aspects such as having traveled to areas considered to be bastions for terrorist, having acquaintances or family ties with known felons, and credit history with questionable history or bankruptcy. Any one of these, or all of these in a person's past, do not mean the individual is a risk to aviation, but the presence in an individual's background could be a precursor to that risk and worthy of interview to assess the risk and to monitor an individual's behavior following the receipt of a badge.

E. PROPOSED METHOD TO MANAGE AVIATION INSIDER THREAT—100 PERCENT EMPLOYEE SCREENING

The consequences of an attack perpetrated by an aviation insider could be disastrous and monumental. An insider (employee) could simply carry a weapon into the restricted area and provide an individual or groups of perpetrators with weapons on the sterile side of the airport after they have been processed by TSA passenger screeners. Once inside the sterile area, the armed perpetrators would have no additional security scrutiny prior to boarding an aircraft. Other means of sabotage could also occur such as placing explosives on aircraft in the cargo holds, damaging flight control or propulsion systems, or secreting other individuals through employee portals undetected. As such, much thought has been given to attempt to eliminate the threat.

Congress, the media, and other groups have expressed concern at the current system. One solution proposed by individuals within congress is 100 percent employee screening. One hundred percent employee screening is defined by the Congressional Committee on Homeland Security in a report directing the Assistant Security of DHS to address vulnerabilities in aviation security by carrying out a pilot program to screen airport workers. In this report, 100 percent employee screening is described as

application “of the same standards as apply to passengers at airport security screening checkpoints” (U.S. House of Representatives, 2007). Individual Congressmen have threatened 100 percent employee screening as a mandated and regulated solution to the dilemma. In some cases, a pilot program for 100 percent employee screening was conducted at several U.S. airports (U.S. House of Representatives, 2007). The Government Accountability Office (GOA) has indicated that current forms of 100 percent employee screening are not practical or realistic. The cost of such a solution would be extraordinary and, in some cases, put commercial airlines out of business. Likewise, the notion that airports could realistically screen their entire population of employees with over 100 percent effectiveness during the course of the working day is impossible to achieve. Any fixed system, process, or procedure, such as 100 percent employee screening, will just be another measure that the highly adaptive insider will learn to manipulate. Once employees learn the process, those that would inflict harm, will learn ways to defeat the screening process.

Airports and other critical infrastructure that have miles of secure perimeter to protect, all have similar vulnerabilities. If an employee is required to go through a screening checkpoint as he/she arrives at work, there is not a measure in place or currently feasible to deny an insider from driving or walking to a remote location on the secure perimeter and passing weapons or other dangerous items over, under or through the perimeter fence. The screening of 100 percent of the employees only determines if they have authorization to be in the restricted area and if they are free of weapons, explosive devices, or prohibited items at the point they are screened. A multitude of other opportunities to acquire contraband are available to an insider following screening. There is not a system that is capable of determining whether they are friend or foe.

Given that insiders are quick to learn how to work around any system that may be put into place; a more sophisticated approach is in order. For an approach to be effective at detecting and deterring an insider, it must be a dynamic system that is based on varying levels of security in a layered fashion, executed in a random manner (Elias, 2009)

F. ENHANCING CURRENT MEASURES TO DECREASE THE INSIDER THREAT TO AVIATION

The current system for employee vetting is foundationally solid. No one has the ability to see into the future or into the mind of a person that is scheming to do ill will; however, certain patterns of behavior can be a precursor indicating a person's willingness to act outside of the law. This behavioral pattern recognition is the strategy employed by aviation security professionals as they attempt to provide access to restricted areas of an airport to those that would contribute to aviation through employment and deny those that have patterns of behavior that cause an authority to question a person's motives for access to restricted areas. A review of an individual's criminal past (CHRC) is a historical, behavioral review; however, there are additional measures and steps that can be built upon or shored up to this foundation.

G. CRIMINAL HISTORY RECORDS CHECKS—FREQUENCY

An individual is required to have a CHRC completed before they are issued their original badge. While the badge is typically valid for a predetermined timeframe (most airport authorities use a two year time frame), the employee is not required to have an additional CHRC completed when his/her badge is renewed. Therefore, this creates blindness for aviation security professionals as they have no built in measures to track an employee's criminal behavior over time. There is a requirement for employees to self-report a conviction of one of the disqualifying crimes but that measure is not effective and will be discussed in greater detail as this narrative progresses. The frequency of a CHRC is an area for consideration.

H. EMPLOYEE SELF REPORTING CRIMINAL CONVICTIONS OF A DISQUALIFYING CRIME

As indicated earlier, an employee that has been convicted of one of the disqualifying crimes is required to self-report the conviction within 24 hours of the conviction to the employer or airport operator. This requirement is deeply flawed for several reasons.

First, there is no obligation for an employee to report being arrested or charged for any crime. Therefore, it is reasonable to believe that an employee that has been arrested of one of the disqualifying crimes will not report the arrest leaving the airport operator without this critical piece of intelligence.

Furthermore, it is reasonable to think that since a secondary or subsequent CHRC is not required once the initial CHRC is completed prior to employment. Moreover, since there is not an automated or likely means for the employee arrest or conviction to come to the airport operator's attention, unless the employee volunteers this career ending information, that employee could maintain his/her employment long term without the airport operator's awareness. This would mean that a high risk individual could have unescorted access to the restricted areas of an airport.

Under the current regulations, criminal prosecution or fines are not likely. As such, combined with the fact the a CHRC is not required following the initial CHRC, the risk to the employee is greater for following the rules as opposed to keeping the conviction a secret.

I. REQUIREMENT TO REPORT ARREST—NOT JUST CONVICTIONS

Another helpful piece of evidence that is not available in every case to the aviation security professional is the presence of arrests related to a CHRC. The disqualifying crimes prohibit the unescorted access of individual's that have been convicted; however, there is no obligation for an employee to report any arrest to the airport operator. The only requirement is to report a conviction of one of the disqualifying crimes. Under the legal system, charges get reduced, adjudicated, or at a minimum, take months and years to litigate. For these reasons, it is important to an aviation security professional's awareness that all arrests are reported and considered into the approval process of unescorted access.

U.S. Customs and Border Protection (CBP) have some similar duties and authorities as it relates to aviation security and access to CBP security areas at airports (19 CFR 122.187). Under this law, CBP has grounds to revoke or suspend access to its secure airport area if the employee has been arrested for, or charged with an offense listed

in Sec. 122.183 (a) (4) and prosecution or other disposition of the arrest or charge is pending. This measure provided to the CBP Port Director allows him/her the ability to act on intelligence that might be detrimental to the integrity of the CBP security area in the best interest of safety and security before final legal measures are complete.

J. LIMITATIONS ON DEPTH OF CRIMINAL HISTORY RECORDS CHECKS—10 YEARS

Another blind spot in the CHRC is the requirement to consider an individual's criminal history for a period of 10 years. While an argument could be made to consider the individual's entire criminal history for the purposes of issuing an airport badge, the more serious concern is the inability to inspect all individual's criminal history over that 10 year period. Aviation security professionals are blinded by crimes that are committed by an individual as either a juvenile or if they have immigrated to the United States during that 10 year period.

Individuals who immigrate to the United States legally are not prohibited from receiving an airport identification badge and having access to secure areas. Therefore, an individual that has committed crimes in another country may not be discovered to have those criminal convictions.

Juvenile criminal records are protected from this review in the interest of not burdening adults with the transgressions of their youth. However, in the case of an 18 year old airport employee, this is another significant blind spot for aviation security professionals in determining the character of those that would be granted unescorted access to secure airport areas. This will be discussed in greater detail later in the section on Juvenile criminal history.

K. AIR CARRIER (PRIVATE SECTOR) AUTHORITIES

Another measure in place, under the authority of 49 CFR 1544, allows airlines (private sector) to be the sole consumer of the individual's CHRC once it has been completed. In this case, the aviation security professional at the airport authority is not allowed to review the criminal history. This allows the private airlines with a primary

interest in the profit of the company to be in conflict with making a decision on unescorted access and profit margins or other interests. The activity of reviewing CHRC of employees has been split between the airport operator and the aircraft operator.

L. MEASURES COMMONLY USED OUTSIDE OF THE AVIATION ENVIRONMENT THAT MAY BE TRANSFERABLE TO FURTHER DISRUPT THREATS FROM INSIDERS

Beyond simply checking an employee's criminal history for patterns of criminal behavior, other checks have the ability to demonstrate behaviors that might indicate an employee's susceptibility to behave outside the law. Those commonly utilized checks include a review of credit history, employment history, personal references, travel behaviors, driving records, Psychological evaluation, and Juvenile Criminal History

1. Credit History

One commonly reviewed and immediately valued measure is a personal credit history review. Credit checks are easily attainable and low cost. Among other virtues, a credit check can assist in providing additional confidence in the individual's identity. While it is possible to possess fraudulent identification documentation, backing up that identity with a history of credit or spending behaviors is more difficult to quickly produce. This adds value to verifying the identity of the individual.

Also, a credit check can provide intelligence on an individual's financial well being. While bankruptcy and other financial challenges do not at face value indicate a person is or could have criminal intentions, it can be one more indication of an individual's desperation. A history of bankruptcy and mounting debt, combined with an individual's criminal history and/or other key indicators, could provide a trained aviation professional the data necessary to deny a badge—or at least monitor the employee carefully if the badge was provided.

2. Employment History

Another source of intelligence that can be added to the review of an individual for potential access to secure areas of an airport is employment history. Reviewing an

individual's employment history over a period of time can reveal behaviors in work place settings that can likely be duplicated in the new work place environment at the airport. Disciplinary actions, terminations, or other actions in employees are indicators of behavioral patterns. Here again, on their own and without sufficient data from other information streams, the behaviors may not be indicative of an individual's propensity to act outside of the law. Even so, combined with other key indicators that are readily available to an aviation security professional, patterns could emerge that are actionable.

3. Personal References

Another easily accessible source of intelligence on individuals is personal references. Personal references sometimes referred to as character reference check allow for those with a more intimate knowledge of the individual to provide insights into the integrity of the individual. While it may be easy to find someone that will provide informal testimony on an individual's character, even sometimes fraudulently, this step forces an individual to identify persons inside the individual's inner circle of colleagues, friends, and associates. These known associates each come with their own background and behavioral patterns that, on their own, may serve to tip the aviation security professional to question the associations and the company the individual keeps.

4. Travel Behaviors

Another useful piece of information that can assist the aviation security professional in determining whether to grant unescorted airport access to an individual is the individual's travel patterns. Specifically, documentation demonstrating an individual's travel history, including international locations that are otherwise regarded as unfriendly towards the U.S. and with a history or harboring, aiding or funding terrorist organizations. The mere fact that a person travels to such an unfriendly country on its own would not be a red flag and cause a badge to not be issued but it might be one of many yellow flags that cumulatively would cause an aviation security professional to deny unescorted access.

5. Driving Record

A person's driving record is another source of identification and intelligence. Here again, while acquiring fraudulent identification is somewhat easy today, having a driving history is not attainable in a matter of days but is acquired over a lifetime. Granted, not everyone has a driver's license, and, for this reason and others, it is not regarded as the final authority on identity or criminal behavior patterns but it is another valuable piece of information in comprising an individual's behavior profile.

On a related note, employee's that operate motor vehicles on the aircraft movement area are not typically required by local laws to have a valid driver's license. However, in the interest of aircraft safety having individuals operating motor vehicles that have questionable driving records, in and around aircraft on the secure side of an airport is not a good practice. Thus, an additional benefit of checking an employee's driving record could improve safety on the airport in the aircraft movement area.

6. Psychological Evaluation

Psychological evaluation is another measure used by employers who are processing applicants for sensitive jobs. Applicants may be required to submit to a psychological evaluation before they can be employed. A psychological evaluation or mental examination is an examination into a person's mental health by a mental health professional, such as a psychologist. A psychological evaluation may result in a diagnosis of a mental illness. It is the mental equivalent of a physical examination and can provide additional intelligence into the overall picture of an individual, including potential for perpetrating violence.

7. Juvenile Criminal History

Finally, criminal history is not inclusive of crimes committed as a juvenile. This blind spot could be problematic for aviation security professionals as airports are employers of many young employees. Currently, the law does not allow the aviation security professional access to an individual's criminal history if the crime was

committed before his or her eighteenth birthday. Therefore, it is plausible that a person could have been convicted of one of the disqualifying crimes before 18 years of age and subsequently applied for unescorted access to restricted areas of an airport at age 20. In this case, the aviation security professional would be unaware of this conviction without the individual volunteering the information that would restrict employment.

Clearly, the vast majority of perpetrators of terrorism are young men. Therefore, while the regulation allows an aviation security professional to consider the last 10 years of criminal history, a 20 year old individual would only have two years of data available for consideration.

M. CONCLUSION

The suspected problems and security vulnerabilities were known by this researcher but considered out of personal control or influence to have a positive impact on the national problem. However, it occurred that the problem while known by many aviation security professionals, the complexities of the problem made it difficult to exquisitely and cumulatively articulate. Therefore, the typical reaction was to discuss or approach the problem in small bites. However, as suggestions are made to add steps or refine processes to further reduce the vulnerability, critics are quick to point out the imperfections within the suggestions. The result is a paralysis among aviation security professionals.

This research does not intend to provide the perfect solution to eliminate the vulnerability. The fact remains, that predicting the future of an individual's behavior criminal intent is not feasible, possible, or likely. That being the case, this research analysis's current methods, looks for new innovations or steps to enhance the ability to manage the threat presented by aviation insiders. This author believes that enhancements to the current method of managing insider threat has been inhibited by the general understanding that no single step or series of steps will eliminate the vulnerability.

THIS PAGE INTENTIONALLY LEFT BLANK

V. RECOMMENDATIONS/CONCLUSION

Based on the findings of the previous chapter, a number of specific recommendations are presented in this chapter, which seeks to mitigate the insider threat to aviation security. Recommendations that promise to produce the most significant impact on mitigating the insider threat, after balancing them against the criteria, including effectiveness, public perception, the cost, and ease to implement, will be summarized in this chapter.

In the previous chapter, it was determined that the current process to vet a potential employee's background had significant value that should be leveraged and enhanced. Furthermore, it was determined that additional enhancements such as a review of credit history, employment history, and travel patterns, would strengthen the current methodology. Each of these additional recommendations will be discussed and evaluated in the following sections.

A. THE BADGING PROCESS

Six specific areas within the current badging process were reviewed: positive identification, CHRC, self-reporting criminal convictions, reporting of arrest, the depth of CHRC, and air carrier authority. It was determined that each area contains opportunities to further enhance existing processes that would deny access to those within the aviation employee group to secure areas based on past behaviors.

1. Positive Identification

Accessing the effectiveness of an airport security badging process begins with establishing whether an employee is legitimate. Absence proof and confidence that the employee/applicant is actually providing his/her actual identity, everything that follows in the badging process is likely to be ineffective in mitigating, in part, the insider threat.

In evaluating the current requirements under federal law for proof of identity, there are some noteworthy gaps. Under the list of documents acceptable for proof of

identity are a school ID card with a photograph and a voter's registration card. These documents are either easily attained through fraudulent means or easily reproduced. In addition, this same federal requirement allows individuals under the age of 18 to present documentation as a means for identification to include a school record or report card, a clinic, doctor or hospital record, or a day-care. Here again the reliability of these documents are unquestionably inadequate as a means to prove identity for the purposes of getting access to secure areas of U.S. airports. It is difficult to imagine that a U.S. airport could potentially allow an employee/applicant to produce a nursery school record as a form of identification.

Other forms of identification used to verify an employee/applicants identity are more traditional, mainstream, and less likely to be reproduced fraudulently. Those include driver's licenses and ID cards issued by government agencies; such as, military ID cards.

School ID cards, voter's registration cards, school records, report cards, clinic/doctor/hospital records and day-care nursery school records should be eliminated from the federal requirements. Elimination of the low quality forms of identification would increase the effectiveness of the employee/applicant vetting process. Requiring higher quality identification is an enhancement that would be readily accepted by the main stream public, would not increase operational cost to aviation, and would be easily implemented. Therefore, this measure will appear as a recommend of this research.

2. Criminal History Records Checks – Increasing Frequency

The current requirement to conduct a CHRC at the beginning of an employee/applicants career at a U.S. airport is a cost effective and accepted baseline measure in evaluating an employee's past behavior as a measure to predict future behaviors. However, failure to require a continued review of an incumbent employee's criminal behavior over the course of what is commonly a multi-decade career is grossly inadequate. Since most U.S. airports have a adopted a badge renewal process that

requires an employee to renew their badge on a two-year interval, this seems to be the ideal time to conduct a follow up CHRC to verify the employee has not been convicted of a criminal offense during this same period of time.

This measure has shown anecdotal evidence of value from partial implementation at DFW airport mentioned earlier; however, it is not without cost to conduct this additional measure. At a minimum, this cost would include a submission fee currently collected by the American Association of Airport Executives (AAAE). The current cost to perform this additional check beyond the initial CHRC would be a minimum cost of $27 per badge for the AAAE to receive the request, process it through the FBI, and return the results to the requesting airport. This is additional cost, when considered against the fact that there are thousands of employees working at U.S. airports that would be included in this enhanced measure, the cost would be significant. For instance, DFW Airport renews approximately 11,000 badges annually.[8] This cost would be approximately $300,000 for just this one airport; however, the cost would typically be passed on to the badge holder or company sponsoring the individuals' unescorted access.

There is other incidental costs that are specific based on local capacity in determining the overall cost of this enhancement. This additional step in the badging process would no doubt increase wait times for badge renewals as the CHRC is run through the formal channels. It could increase headcount for employees in the badging office in order to keep pace with the demands that would result from the additional step.

Despite the significant cost that would likely result from this enhancement, the additional situational awareness gained from a CHRC is not possible to attain through another measure. Increasing frequency of the CHRC to every two years is a proven, effective measure, would be easily implemented and would have broad public support. Regardless of the cost to execute this enhancement, this measure is believed to be a valuable step and will therefore appear as a recommendation from this research.

[8] Information obtained by author through databases with DFW Airport not available to the public.

3. Self Reporting Criminal Convictions—Incentivizing

There are currently no incentives for employees to self-report criminal convictions of a disqualifying crime as required by federal law. Self-reporting such a fact would likely end an aviation employee's career at U.S. airports. While the federal requirement is explicit that an employee is required to report the conviction within 24 hours, it is unlikely this would be the case.

Therefore, it is essential that regulators take steps to hold individuals accountable for failing to report such convictions. In addition to criminal prosecution for failing to self-report, a civil process should be exploited to fine the individual for the failing. These additional measures should be implemented to hold the individual employee accountable for failing to self-report but also sends a message to the balance of aviation employees that failing to following the requirements results in harsh consequences both criminally and financially.

This measure has an increasing value if the recommendation to increasing the frequency of the CHRC is not adopted. This increased frequency would serve to uncover employees that have failed to self-report. Two areas of improvement are in order to minimize this vulnerability. First, rechecking an employee's CHRC every 2 years would provide an automated means to bring the employee's behavior to the attention of the airport operator. Second, imposing financial and criminal sanctions on employees that fail to self-report would provide incentives for employees to report the convictions before they were found out during the normal CHRC process and limit further their criminal and financial liability.

This measure would improve the overall effectiveness of the process, be widely understood and accepted by the public, be easy to implement. Fines can help offset the cost to litigate the measure. For these reasons this measure will be included in the recommendations.

4. Reporting of Arrest—Not Just Convictions

While the requirement to self-report criminal convictions for disqualifying criminal offenses is a step in the right direction, the fact is this is only a small step in improving an airport operator's situational awareness of an employee's criminal behaviors. In today's world, individuals are arrested only to commonly have the charges dropped, deferred, or otherwise reduced. In addition, the legal process is a time consuming process, particularly in the arena of criminal prosecution.

That being the case, airport operators are operating under a false sense of security if they are unable to have the full benefit of an employee's criminal activities regardless if they are alleged for not. While an arrest on its own is not normally sufficient information for an airport operator to terminate an employee's employment, it would, in many cases, provide the airport operator with more timely information that might cause an employee to be reassigned to less security sensitive activities, pending disposition of the charge. In addition, multi-arrests, regardless of convictions, would warrant a review of the employee's access rights and, subsequently, a reassessment of those access rights.

Requiring employees to self-report arrest, not just convictions for disqualifying criminal offenses, is complementary to increasing frequency of the CHRC to a two-year interval and to the measure to incentivizing self-reporting of convictions. If an employee has confidence his/her behavior will be disclosed automatically at some interval, during the badge renewal process, and is aware that additional criminal and financial consequences are likely to occur if he or she fails to abide by the requirement, his/her likelihood of self-reporting the arrest is dramatically increased.

It is also noteworthy that the U.S. Customs and Border Protection has a similar requirement to report arrest within a 24-hour period for access to the secure areas of international airports in the areas they control (Federal Inspection Stations). For the same reason, this provision is available to the CBP Port Directors at airports, this authority should be added to the tools available to the airport operator.

This enhancement to the current methods within the federal requirements would require an employee to self-report arrests and as such, would increase the effectiveness of

the measure, would not be an additional expense, it is easy to implement, and would be regarded by the public as an appropriate measure for employees working in a secure aviation environment.

5. Depth of Criminal History Records Checks—10 Years

As discussed previously, the requirement that disqualifies an employee/applicant from unescorted access to secure areas of an airport based on criminal convictions for a disqualifying crime in the last 10 years is reasonable, prudent, and actionable; however, this requirement assumes the crime history is easily attainable. This is the case for most U.S. citizens or individuals that have lived in the U.S. or a country with friendly ties to the U.S. for the last 10 years. However, this is not the case of employee/applicants that are from countries that do not share information with U.S. law enforcement readily. In these cases, it is difficult, if not impossible, to determine an individual's criminal background with the same degree of confidence. As such, a policy revision that recognizes this inability to gather actionable information is necessary. A more robust investigation is warranted and the policy should reflect narrative to reconcile the inability to verify information for the full 10-year term.

In addition, consideration should be given to allow aviation security professionals the authority to consider juvenile crimes in the issuances on an airport identification badge. The policy should have requirements such as:

- Verifiable 10 years of history
    - Must be U.S. citizen for 10 years, or,
    - Must have lived in a country that will share criminal data during the 10 year period, or,
    - Include juvenile history for employees 27 or younger.

6. Eliminating Air Carrier (Private Sector) Authorities

Forty-nine CFR 1544 currently allows air carriers, under certain conditions, to be the consumer of CHRC for their individual employees/applicants. This authority allows air carriers to review CHRC and make employment decisions based on the employee's

criminal past. With many different air carriers allowed this authority is it unclear how they apply the authority. Where employers under the federal requirement are allowed to make judgments on the potential employee/applicant threats to aviation based on this review, they hardly seem objective enough to make this judgment when dealing with their own employees. The airport operator is left without situation awareness as to the criteria applied by the air carriers in making that decision.

It is more efficient and effective to have the process of reviewing an employee/applicant's CHRC in a consolidated fashion by the airport operator in concert with local law enforcement. This consolidation under the airport operator provides for a higher degree of situational awareness across the full spectrum of employees working at an airport in order to more effectively manage the aviation security and the risks of aviation insiders.

The process of employee badging is not increased in steps due to the air carrier involvement in the CHRC step, this single step is merely completed by the air carrier instead of the airport operator. However, there may be incremental additional cost involved in implementing this measure through consolidation. Air carriers pick up some savings internally by completing this step, although it is not completely clear how much. Even so, the cost savings, when balanced against the air carrier cost to staff up in order to complete the internal review, is not considered to be significant.

Regardless of the actual cost to implement this measure, the overall effectiveness of the badging process in total is considered to be very significant. In addition, the implementation of the measure is considered to be easy to implement and the public perspective is expected to be highly favorable for such a policy revision.

Table 2. Enhancing Current Measures

	Effectiveness	Public Perception	Cost	Implementation Ease
Position ID	High	Favorable	Low	Easy
CHRC Frequency	High	Favorable	High	Easy
Self Report	High	Favorable	Low	Easy
Report Arrest	High	Favorable	Low	Easy
CHRC Depth	High	Favorable	Low	Easy
CFR 1544	High	Favorable	High	Difficult

B. ADDITIONAL MEASURES BEYOND CRIMINAL BEHAVIORS

The review of an individual's crime behaviors is probably one of the most reliable methods to determine the potential for an employee to act outside of the confines of the law in the future. (Bartal & Bartal, 2007); however, there are other evaluations that present opportunities to evaluate an individual's behavioral patterns. Other types of evaluations, such as personal credit history, employment history, personal references, travel patterns, driver's license records, and psychological evaluation, are common in some preemployment settings when an individual applies for a position that requires a certain amount of confidence in the individual's integrity. The other evaluations types will be discussed and evaluated using the criteria mentioned in Table 3.

1. Credit History

An individual's credit history is commonly used in determining employability. An individual's financial health is one indicator that the individual is responsible in addressing his or her financial obligations. From a security perspective, the presence of derogatory financial data, or in more extreme cases bankruptcy, may lead to desperation and illegal activities to overcome the financial deficiency.

Credit histories are easily attainable through commercial services for a nominal fee. Public perception is favorable for such a measure given the common utilization. In addition, the ease of implementation and the effectiveness of the measure, when combined with other forms of background check is favorable. For these reasons, credit

history should be checked on individuals receiving permission to have unescorted access to secure areas. In addition, a credit history check should be completed initially and each time the badge is renewed.

2. Employment History

Another commonly utilized method of determining an individual's employment is a check of previous work history. When employers review an individual's work history, they are typically looking for red flags that might indicate the individual is not a good fit for the organization. Matters such as low performance, disciplinary actions, or even job terminations are indicators that make the employer explore other attributes, either in writing or during interviews, areas of concern that may present a work place problem.

While it is a common practice for many employers to check employment history prior to an offer of employment and an application for unescorted access being requested, work history is not currently shared with the airport operators as they attempt to evaluate the level of risk posed by the employee.

The cost associated with this additional detail is moderate but the ability to raise situational awareness among the aviation security professionals is highly valuable. Therefore, while cost is nominal, the effectiveness is considered to be high when implemented in conjunction with other background measures. The public perception would be favorable as employment history is a common benchmark in today's work force and the expectation is already in place. The implementation is considered very easy. Employment history checks are recommended for those that are requesting unescorted access to secure areas.

3. Personal References

Most applications for employment require an applicant to provide personal references. Personal references are generally collected from individuals that have extended personal and work relationships with the applicant. In many cases, those selected by an applicant as a personal reference have been prebriefed as to what information the applicant would like the individuals to give to the potential employer.

However, there are those occasions where a personal reference will be honest if asked about the applicants personal and work related behaviors. This is one of those questions that if not asked relevant information might be missed that could aid the employer in determining suitability for employment.

Also, personal references are frequently provided that are currently employees of the organization where the applicant is considering employment. Having a personal reference coming from within the organization is viewed by the employer as beneficial since the personal reference; incumbent employee is more accountable for the reference that outside the organization. An incumbent employee that provides a personal reference for an individual that is later hired and determined to be a poor performing has his or her integrity on the line. As such, an incumbent employee is a good source for honest feedback in many cases.

From the perspective of an aviation security profession, personal references offer several potential benefits. First, just as the employer has the benefit of feedback from someone who has an extended personal or work history with the applicant, this can bear similar fruit for the aviation security professional. If the person is considered a threat to aviation by the personal reference, there is a chance this will be communicated during an interview with the personal reference.

In addition, there is a second benefit that is more subtle but just as powerful. An applicant that list as his or her personal references individuals that themselves have questionable integrity would be a red flag for an aviation security professional. A personal reference that was a known gang member, for instance, would be a red flag that would cause an aviation security professional to take note. Here again, these linkages between applicant and a personal reference that is an incumbent employee make the connection even more important and easier to review. An incumbent employee, who has been adequately vetted and approved to have a badge, is one who the aviation security professional has the ability to go back and research previous data bases looking for other known associates or suspicious behaviors.

Requiring personal references for the purpose of being granted unescorted access to secure areas is considered to be minimal in cost, easy to implement, and favored by the public. In addition, the effectiveness of this measure, in conjunction with others recommended, is considered very high.

4. Travel Patterns

Over the last several years, the law enforcement community has been concerned and seen evidence of homegrown terrorist. United States citizens who have turned to radical Islamic beliefs and conspire to attack the U.S. on behalf of foreign-based terrorist are just one form of a homegrown terrorist. In many cases, homegrown terrorists have made multiple trips to foreign locations to obtain orders or participate in training to carry out a terrorist mission.

U.S. citizens that travel to foreign locations are required to have a passport in order to travel. As such, their travel is recorded and can aid the aviation security professional is seeing the entire picture of an individual's motivations. Since a passport is considered, in accordance with federal requirements, to be identification that is both proof of identity as well as employment authority, this form of documentation is commonly provided by applicants desiring unescorted access.

Requiring an applicant to report previous travel outside of the U.S. is considered to be easy to implement, low cost, and favored by the general public. Furthermore, the effectiveness is deemed high as it adds to the applicants overall profile and is useful when used in conjunction with other measures. For these reasons, it is recommended that travel behavior is required to be reviewed initially and each time a badge is renewed.

5. Driving Record

An individual's driving record is frequently a requirement for employment particularly when the position being applied for is one that requires a driver's license and driving is an essential job function. In addition to validating that an individual has current and legitimate license to drive a motor vehicle, it has additional benefit to the employer by demonstrating past driving behaviors that could cause an employer to reject

the applicant. If the position is one that requires a fair amount of driving, employing someone that has numerous offenses for driving while intoxicated, speeding, or other moving violations may not be a good business decision.

Likewise, requiring a review of an applicant's driving record has merit for the aviation security professional. One such benefit is that despite the relative ease associated with fraudulently producing a driver's license, fabricating a fictitious driving record is much more difficult, particularly if the applicant has been licensed for several years. Therefore, the benefit is one relating back to confirming identity discussed earlier. Second, driver's license records indicate last registered address that could be different from the application and raise questions for the aviation security professional.

Finally, many of the employee's that have unescorted access to secure areas drive vehicles on the secure ramp next to and around commercial aircraft. Individuals that have an extensive history of unsafe driving should be restricted from these close and high value encounters.

A review of driving records can be easily attained, at very low cost, and would be considered favorably by the public. In addition, it would be very effective when employed in conjunction with the other measures discussed in the research and is recommended as a condition of access to secure areas.

6. Psychological Evaluation

Psychological evaluation is another measure employed in some cases during preemployment. Typically, this measure is reserved for employment in areas where high levels of mental health are considered significant. Job fields such as law enforcement are such positions due to the potential for litigation or life safety.

While this measure has a place in the approval for an applicant to have unescorted access to secure areas, it is not recommended for adoption for several reasons. The sheer number of employees that would have to be psychologically screened would be so high it

would overwhelm the mental health system. Just requiring police officers and other high security, high risk employees screened requires significant time to schedule and have completed.

In addition the cost for such a high level of professional screening would make the cost benefit unbearable for most aviation employers. While the public would support such an extreme measure, it would be very difficult and costly to implement. The effectiveness is likely to be positive, but the other value streams would not support implementation. Therefore, this measure if not being recommended as part of this research.

Table 3. Additional Needs

	Effectiveness	Public Perception	Cost	Implementation Ease
Credit History	High	Favorable	Low	Easy
Employment History	High	Favorable	Low	Easy
Personal References	High	Favorable	Low	Easy
Travel Patterns	High	Favorable	Low	Easy
Driving Record	High	Favorable	Low	Easy
Psychological Evaluation	High	Favorable	High	Difficult

C. RECOMMENDATIONS FOR FUTURE RESEARCH

The preceding research takes a very broad and misunderstood vulnerability and synthesizes it into an easily understandable and actionable product. However, it is important to acknowledge that the issue is a highly complex one that has no single answer resolving the vulnerability. The size of the problem is compounded by the number of aviation insiders with access to secure areas, and the uniqueness of individual airports creates limitations for this author in addressing the problem from a national perspective.

This research offers a number of steps that can be taken collectively or incrementally that will aid in closing the gaps aviation insiders could exploit with some degree of ease within the current system. It is recommended a pilot program, involving several airports of various sizes, be implemented to test the viability of the measures recommended in this thesis.

Implementation costs for each measure will need to be more carefully calculated across the aviation domain as the information available to this author, while considered to be reliable, may not be repeatable at the over 400 airports in the United States. Cost could be captured by a study or from the pilot program previously recommended.

D. CONCLUSION

Based the proceeding recommendation review, the following conclusions are provided for implementation.

1. Changes to the Current Badging Process

1. Eliminate proof of identification documentation that is not issued by the federal or state government.
2. Implement a recheck of criminal history records with each badge renewal.
3. Implement criminal and civil penalties for employees failing to self-reporting convictions of disqualifying crimes.
4. Require aviation employees with access to secure airport areas to report all arrests to the airport operator.
5. Implement a requirement that criminal history records checks must include an ability to verify information for the full 10-year term and include juvenile crimes during the 10 year period. The policy should include the following provisions:
    - Must be U.S. citizen for 10 years,
    - Must have lived in a country that will share criminal data during the 10-year period, or
    - Include juvenile history for employees 27 or younger.

6. Eliminate private sector (air carrier) authority to have employers unilaterally authorize badging of employees following reviewing of CHRC. Require all CHRC be reviewed and approved by the airport operator as a single authority.

2. Additional Measures Not Part of the Current Process

In addition to the measures to the existing process, the following measures are considered effective and are recommended for implementation.

1. Conduct a credit history report on all employees that require access to secure areas initially (before employment) and each time the badge is renewed.
2. Complete a check of employee/applicant's work history for the last 10 years for new employees.
3. Require all new employees to provide at least three personal references.
4. Require all new employee/applicants and all incumbent employees with access to secure areas to provide full disclosure of all travel outside of the United States.
5. Require airport operator driving history review of all new employee/applicants and all incumbent employees with access to secure areas.

E. SUMMARY

It is well documented and, above all obvious, that the threat imposed by aviation insiders, armed with knowledge and access is a vulnerability facing U.S. aviation. Although there is a clear threat, the way forward in managing the threat has been poorly researched and acted upon. The complexities of the aviation insider threat frame the problem in an overwhelming manner.

Further compounding the issue and diminishing action is that when suggestions are made to add steps or refine processes to further reduce the vulnerability, critics are quick to point out the imperfections within the suggestion. The result is a paralysis among security specialists. Typical of many aspects of government, this is an issue that those responsible for aviation security at all levels of government seem to lack the courage or expertise to face in a proactive manner.

This research does not intend to provide the perfect solution to eliminate the vulnerability. The fact remains that predicting the future of an individual's behavior or criminal intent without error is not feasible or possible. That being the case, this research analysis' current methods, looks at new innovations and steps to enhance the ability to manage the threat presented by insiders. This research constitutes the most comprehensive body of research on the topic of insider threat in the aviation environment. Furthermore, it provides recommendations that are reliable and actionable in combating the overwhelming nature of the issue. As such, it provides the single best roadmap to address the issue.

Unfortunately, this vulnerability may only be fully recognized and studied with steps taken to minimize the risk after an attack occurs. The hope of this author is that through this research, it will bring awareness to the issue at the right levels of government and that actions will begin to be studied and implemented before the first attack occurs.

LIST OF REFERENCES

12 charged in sting at New York Airport. (2009). Retrieved December 21, 2009, from www.airportbusiness.com/online

Aviation transportation system security plan. (2007, March 26). Retrieved January 2, 2010, from www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf

Bliss, J. & Blum, J. (2009). *Napolitano says coordination key to tracking Al-Qaeda backers.* Retrieved October 13, 2009, from www.bloomberg.com/apps/news?pid=20601103&sid=ap08muY1VMb8

Collins, B. M. (2009). *Intelligence briefing.* Presentation to the Director of Public Safety, Houston Airport System, Public Safety and Technology Division, Houston.

Department of Transportation. (2002). *Civil Aviation Security Rules, Final Rule 49 CFR 1542*. Washington, D.C.: U.S. Government Printing Office.

Elias, B. (2009). *Airport passenger screening: Background and issues for Congress.* Washington, D.C.: U.S. Government Printing Office.

Kilpatrick, S. (2008, September). Refining insider threat profiles. *Security Magazine*, *45*, 9.

Miller, E., & Dover, M. (1998). *An analysis of federal airport and air carrier employee access control, screening, and training regulations.* Mater's thesis, Naval Postgraudate School, Monterey, CA.

National Commission on Terrorist Attacks upon the United States . (2004). *Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Co.

National strategy for aviation security. (2007, March 26). Retrieved January 2, 2010, from www.dhs.gov/xlibrary/assets/laws hspd aviation security.pdf

Noonan, T. & Archuleta, E. (2008). *The insider threat to critical infrastructures: The National Infrastructure Advisory Councils final report and recommendations.* Retrieved November 27, 2010, from: http://www.dhs.gov/xlibrary/assets/niac/niac_insider_threat_to_critical_infrastructures_study.pdf

Office of Inspector General, Department of Homeland Security. (2008). *TSA's security screening procedures for employees at Orlando International Airport and the feasibility of 100 percent employee screening.* Washington D.C.: U.S. Government Printing Office.

Office of Intelligence and Analysis and Federal Bureau of Investigation. (2007). *Joint homeland security assessment, recent terrorist plots highligh insider threat.* Unclassisfied/Fort Official Use Only: Department of Homeland Security.

Perimeter security: Much is yet to be done. (2009). Retrieved October 25, 2009, from www.homelandsecuritynewswire.com/single.php?id=8560

Price, J. (2007, June/July). Ramp clampdown. *Airport Magazine* , pp. 43–47.

Randazzo, M. (July-September, 2008). Reducing violence and sabotage in airports: The use of threat assessment to manage employee threats. *Airport Management, Volume 2* , 325–335.

Temp agency owner sentenced for aiding illegals. (2009). Retrieved October 1, 2009, from www.chicagotribune.com/news.chi-ap-il-airportworkersarr

Transportation Security Administration. (2008). *Transportation Intelligence Gazette - Clean Skins, Lone Wolfs, and Insiders.* Unclassified/For Official Use Only.

Transportation Security Administration, Department of Homeland Security. (2007, April 19). *Airport security: The necessary improvements to secure America's Airport:s Prepared statement by Bennie G. Thompson, Chairman, Subcommittee on Transportation Security and Infrastructure Protection.* Retrieved October 29, 2009, from U.S. House of Respresentatives Committee on Homeland Security: www.homeland.house.gov/Hearings/index.asp?ID=35

Transportation Security Administration, Office of Intelligence. (2009). *Sterile Area Threat Assessment: "The Insider."* Unclassified/For Official Use Only.

TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening. (2008). Department of Homeland Security, Office of Inspector General.

U.S. Government Accountability Office. (2009). *Aviation Security: A national strategy and other actions would strengthen TSA's efforts to secure commercial airport perimeters and access controls* (GAO-09-399). Washington, D.C.: U.S. Government Printing Office.

U.S. Government Accountability Office. (2004). *Aviation security: Further steps needed to strengthen the security of commercial airports and access control* (GAO-04-728). Washington, D.C.: U.S. Government Printing Office.

U.S. House of Representatives. (2007). Directing the Assistant Secretary of Homeland Security to address vulnerabilities in aviation security by carrying out a pilot program to screen airport workers with access to secure and sterile areas of airports, and for other purposes. (pp. 110–482). Washington, D.C.: U.S. Government Printing Office.

Weikel, D. (2008, September 5). *LAX Tightens Security Measures After Alleged Smuggling.* Retrieved September 5, 2008, from LA Times: mobile.latimes.com/detail.jsp?key=179165&ull=1

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California